UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/259,620	02/26/1999	JAMES Q. MI	INTL-0160-US	5503

7590 03/31/2003

TIMOTHY N. TROP
TROP, PRUNER, HU & MILES
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER
MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
2132	13

DATE MAILED: 03/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/259,620	**Applicant(s)** MI ET AL.
	Examiner Douglas J. Meislahn	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2003* .

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) □ Interview Summary (PTO-413) Paper No(s). _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: .

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 28 January 2003 that amended claims 1, 3, 6, 10, 21, and 23, cancelled claims 2 and 7, and added claims 27-37.

Claim Objections

2. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When claims are canceled, the remaining claims must not be renumbered. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claims 36 (the second one) and 37 have been renumbered, respectively, as claims 37 and 38.

Response to Arguments

3. Applicant's arguments filed 28 January 2003 have been fully considered but they are not persuasive.

With respect to claims 1, 3-6, 8, 9, and 21-24, applicant opines that the identifier in Claus et al., which is sometimes described as a personal identification number, cannot be related to a processor's identifier. Applicant provides no reasoning or evidence to support this assertion. As Claus et al. say in lines 11-13 of column 5, the personal identification number stored on a smart card is unique to that smart card. Thus, the personal identification number is unique to the microprocessor (see figure 5, element 560) in the smart card. As such, applicant's assertion is demonstrably false.

Applicant ignores the teachings of the Lee et al. reference, which provides motivation to combine and teaches elements that applicant argues are absent from the prior art. Applicant's comment that the result of modifying Claus et al.'s invention would be "unsatisfactory" is built on the false premise that identifying a smart card cannot identify a person. As is evident from element 561 of Claus et al.'s first figure, access to the unique identifier on the card is guarded. Thus, the unique identifier on the smart card, be it a processor serial number or personal name, identifies any individual who knows the password and the unique identifier.

In regard to claims 10-14, 25, and 26, applicant contends that neither Zdepski nor Schneier suggests selective encryption authorization based on an identification. However, the certificates taught by Schneier are an identity-based verification, and, in case of lack of verification, the key associated with the certificate would not be used. This reads on applicant's selective encryption authorization.

With respect to claims 15-20, applicant states that neither Claus et al. nor Schneier shows the first clause of the claim. Claus et al. has been shown to teach reception of a request for identification.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re*

Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the examiner clearly pointed out that Schneier's disclosure teaches a method that frustrates malicious parties' ability to recover a message or key from a message/key combination.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 3, 6, 8, and 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. in view of Lee et al. (5774544).

Figure 1 of Claus et al. shows a second computer (element 500) receiving a request for identification (step 3) from a first computer (element 700). ID_n is retrieved from memory (550) and sent to the first computer. A cryptogram of ID_n (S_n) is further encrypted with a key shared with the first computer (see figure 2) by element 563. In step 4 the encrypted (or hashed) identifier is returned to the first computer. S_n uniquely identifies the second computer because it is systematically derived from a value unique to element 500 (see lines 11-15 of column 5). A smart card is a computer because it comprises a processor and memory (see lines 33-34 of column 2). See also Claus et al.'s abstract. They do not say that the unique identifier is a microprocessor number. In lines 12-23 of the first column, Lee et al. say that using serial numbers identifying microprocessors allows for better tracking of a hardware component. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use microprocessor numbers, as taught by Lee et al., for the unique identifier in Claus et al. in order to improve control of Claus et al.'s smart cards.

6. Claims 4, 5, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. and Lee et al.

Claus et al. show a computer authenticating itself by supplying an encrypted version of a unique identifier to an authenticating computer. The only information shared by both the first and second computers is E_2, which includes a key. The origin of E_2 is vague, but generally it is said to have been programmed into the smart card during manufacture. The challenge number generator used in Claus et al. is capable of producing truly random numbers and can thus be used to generate encryption keys. With respect to claims 4 and 9, Claus et al. do not state that the key used to encrypt the identifier is received from the authenticating computer. Official notice is taken that it is old and well-known to minimize the number of parties who have access to secret keys, such as those used in E_2 in Claus et al. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for the authenticating entity in Claus et al. to generate the key used in E_2 and send it to the smart card, thereby increasing security by keeping the parties privy to the key to a minimum.

With respect to claim 5, figure 6 in Claus et al. shows a networked environment, in which the two computers communicate via a public switched network. Communications over public networks render obvious web site addresses. As mentioned above, the only information that the two computers share is E_2. Claus et al.

do not say that the key indicates an address of a web site. However, as the key (with its associated, generic algorithm) is the only shared piece of information, the web site address is necessarily indicated by the key. In other words, the one-to-one correspondence of the key to the host computer (element 600), mandates that the key is indicative of the web-site address.

7. Claims 10, 11, 13, 14, 25, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zdepski et al. (5825884) in view of Schneier (*Applied Cryptography*) and Lee et al.

In lines 64-67 of column 4, Zdepski et al. talk about encrypting a platform's identifier with a recipient's public key. In the following column, this cryptogram is sent to the recipient. They do not say that any steps are taken to ensure that the public key is authentic or that the identifier uniquely identifies the platform. On pages 185-186, Schneier teaches certificates as a means to "thwart attempts to substitute one key for another". This is a type of verification. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to verify the public key used in Zdepski et al. to avoid undesired key swaps as taught by Schneier.

In lines 12-23 of the first column, Lee et al. say that using serial numbers identifying microprocessors allows for better tracking of a hardware component. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use microprocessor numbers, as taught by Lee et al., for the unique identifier in Zdepski et al. in order to improve control of Zdepski et al.'s platforms.

8. Claims 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, Zdepski et al., and Lee et al. as applied to claims 1 and 11 above, and further in view of Linehan (6327578).

Zdepski et al., Lee et al., and Schneier show sending identifiers encrypted with a recipient's verified public key. They do not say that the key indicates an URL address. In lines 14-20 of column 5, Linehan teaches including an URL in a certificate. Thus the public key would indicate an URL address. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to follow Linehan's example and include an URL address in the certificate of Schneier associated with the public key in Zdepski et al. This ties the key to a specific entity.

9. Claims 15, 16, 18-20, 27, 30, 31, 34, 35, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. and Schneier.

Claus et al. show a computer authenticating itself by supplying an encrypted version of a unique identifier to an authenticating computer. They specifically teach encrypting with DES, but say, in lines 8-12 of column 8, that other enciphering computations could be used. They do not say that the encryption is a keyed hash. At the bottom of page 458, Schneier discloses keyed hashes with differing presumed security levels. In the simplest embodiment, the keyed hash is H(K, M). Keyed hashes curtail the ability of a malicious party to uncover the original K and M from the hash. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the keyed hashes taught by Schneier as the enciphering computation in Claus et al., thereby combating unwanted disclosure of the identifier and the key. As is apparent from the equation H(K, M), K and M are interchangeable. Thus, Claus et al.'s key is encrypted with the identifier, as per claim 15. For security reasons, the hash algorithm H would be assumed to be collision-resistant, non-commutative, and one-way.

10. Claims 17, 28, 32, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. and Schneier as applied to claim 15 above, and further in view of Lee et al.

Claus et al. and Schneier show a computer authenticating itself by supplying a key encrypted with an unique identifier to an authenticating computer. They do not say that the unique identifier is a microprocessor number. In lines 12-23 of the first column, Lee et al. say that using serial numbers identifying microprocessors allows for better tracking of a hardware component. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use microprocessor numbers, as taught by Lee et al., for the unique identifier in Claus et al. in order to improve control over Claus et al.'s smart cards.

11. Claims 29, 33, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Claus et al. and Schneier as applied to claims 27, 31, and 35 above, and further in view of Linehan.

Claus et al. and Schneier show a computer authenticating itself by supplying a key encrypted with an unique identifier to an authenticating computer. They do not say that the key indicates an URL address. In lines 14-20 of column 5, Linehan teaches including an URL in a certificate, which can be used to authenticate a key. Thus the key indicates an URL address. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to follow Linehan's example and include an URL address in a certificate associated with the key in Claus et al. This ties the key to a specific entity.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703)

746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J. Meislahn
Examiner
Art Unit 2132

DJM
March 26, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100